ManHunt Smart Agent for Cisco™ IDS 4.0 Installation Guide

symantec™

ManHunt Smart Agent for Cisco IDS 4.0 Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 4.0

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, Symantec AntiVirus, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT (SMART AGENT)

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Software utilize content which is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates which Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

About ManHunt Smart Agent for Cisco™ IDS 4.0

The ManHunt Smart Agent (MSA) for Cisco IDS 4.0 enables Symantec ManHunt to receive events in real time from the Cisco IDS 4.0 sensor through Cisco Threat Response (CTR). The MSA converts these events into the ManHunt event format and then sends the events to a ManHunt node for aggregation and correlation with all other ManHunt events. The MSA also enables you to set response policies for Cisco events in the ManHunt Policy Configuration interface.

See the *Symantec ManHunt Administration Guide* for instructions on creating response policies.

System requirements

The MSA for Cisco IDS 4.0 requires the following:

- CTR installed on a separate host running Windows 2000
- Cisco IDS 4.0 sensor
- One of the following:
  - Symantec ManHunt 3.0 installed on Solaris 8 SPARC or Intel, or Red Hat Linux 8.0 (with kernel version 2.4)
  - Symantec ManHunt 2.2 patch 2 installed on Solaris 8 SPARC or Intel

Note: Patch 2 is required for ManHunt 2.2 to enable you to properly view event information from MSAs. You can download the patch at: http://www.symantec.com/techsupp/enterprise/products/manhunt/manhunt_2.2/files.html.

To find out which ManHunt patches have been installed, look in the `<ManHunt_inst_root>/patchlevel` file. The content of the patchlevel file will include the entry `1:2.220.02:ManHunt patch 2.220.02` if you have patch 2 installed. If you do not have a patchlevel file, no patches have been installed.

Setup overview

You can set up the MSA for Cisco IDS 4.0 in five basic steps.

To set up the MSA for Cisco IDS 4.0

1. Set up the Cisco meta data.
   See "Setting up the Cisco meta data" on page 2.
2. Set up the Cisco IDS 4.0 appliance.
   See "Setting up the Cisco IDS 4.0" on page 4.
3. Set up CTR.
   See "Setting up CTR" on page 4.
4. Set up the MSA for Cisco IDS 4.0.
   See "Setting up the MSA for Cisco IDS 4.0" on page 5.
5. Start the MSA for Cisco.
   See "Starting and stopping the MSA" on page 11.

Setting up the Cisco meta data

The Cisco meta data enables you to create response policies and display detailed event data.

Setting up the Cisco meta data involves two steps:

- Installing the Cisco meta data
- Configuring Symantec ManHunt

Installing the Cisco meta data

You must install the Cisco meta data on the ManHunt node that you log into from the ManHunt console, typically the primary master node. This enables you to create the MSA for Cisco external sensor node, create response policies for Cisco events, and display Cisco event data in the ManHunt console.

In addition, you must install this meta data on the ManHunt node that will receive the Cisco event data from the MSA for Cisco (if different from the master node).

Note: You must log on as root to install the Cisco meta data.

To install the Cisco meta data

1 Place the CD in the CD-ROM drive; mount the volume if necessary.

2 Change to the CD directory, and run the following command:

```
cd Cisco40MSA_MH<version>/install/<platform>
```

where `<version>` is `22` or `30`, and `<platform>` is `linux`, `solaris8-intel`, or `solaris8-sparc`.

3 Run the following command:

```
./install-md.sh
```

4 Ensure that the meta data file to be installed begins with `cisco` and ends with the `.md` file extension. If you have old meta data files, you can choose to either delete or archive them. Do one of the following:

- To delete the old meta data files, type `delete` and press **Enter**.
- To archive the old meta data files, type `archive` and press **Enter**.

5 When prompted to restart ManHunt, type `y` and press **Enter**. You must restart ManHunt to incorporate the new meta data.

If this is the ManHunt node used for administration, quit and restart any ManHunt consoles connected to the node to enable the consoles to incorporate the new meta data.

Configuring Symantec ManHunt

To enable communication between ManHunt and the MSA for Cisco, and to be able to set ManHunt response policies for Cisco events, you must create an external sensor object in the ManHunt topology tree for the host on which the MSA for Cisco is installed.

To add an external sensor object

1 On the ManHunt console Monitored Devices tab, do one of the following:

- Right-click **External Sensors** or **Location**, and select **Add External Sensors** from the pop-up menu.
- Right-click an existing external sensor object, and click **Edit** from the pop-up menu.

2 In Add External Sensor or Edit External Sensor, enter a descriptive name of up to 39 characters for the device. This name will appear in the topology tree.

3 Enter a customer ID of up to 39 characters long.

4 Enter the IP address for the device.

5 From the pull-down list, select `CISCO`, which is the Event Receiver that will receive this event data.

6 Set the EDP passphrase of between 8 to 64 characters long, inclusive.

Symantec ManHunt communicates with Smart Agents over an Event Dispatch Protocol (EDP) proxy.

Note: In order to enable a Symantec ManHunt node to receive event data from an MSA, the MSA must share an EDP passphrase with the Symantec ManHunt nodes. If the EDP passphrase element does not appear active, use the `edppwd` tool in the `<MH inst directory>/tools` directory to change the passphrase.

7 In Description, enter an optional description of up to 255 characters, and click **OK** to add the object.

Caution: Click **Topology** > **Save Changes** before quitting the ManHunt console. Any unsaved changes will be lost upon quitting the console.

Note: If you want Symantec ManHunt 3.0 to be aware of each device interface, add an interface object to each device in the topology tree.

See the *Symantec ManHunt Administration Guide* for more information.

Setting up the Cisco IDS 4.0

Setting up the Cisco IDS 4.0 involves configuring Cisco IDS 4.0.

Configuring Cisco IDS 4.0

MSA for Cisco IDS 4.0 receives events from Cisco IDS 4.0 through CTR. In order to send and receive event data properly, CTR must have access to Cisco IDS 4.0. The address of the CTR host must be included in the Access Control List on the Cisco IDS 4.0 appliance.

See the *Quick Start Guide for the Cisco Intrusion Detection System Version 4.0* for more information.

Setting up CTR

CTR sends event data to the MSA. CTR must be installed on a separate computer running Windows 2000.

Setting up CTR involves three steps:

- Installing CTR
- Configuring CTR
- Setting up SNMP settings

Installing CTR

Before installing the MSA for Cisco, install CTR on a separate computer running Windows 2000. CTR sends event data to the MSA through Simple Network Management Protocol (SNMP) traps.

See the *Cisco Threat Response User Guide* for the installation procedure and for more information on this product.

Configuring CTR

You must configure CTR to receive event data from the Cisco IDS 4.0 sensor to send to the MSA through SNMP traps.

See the *Cisco Threat Response User Guide* for the configuration procedure and for more information.

Setting up SNMP settings

The SNMP traps send the event data from the CTR to the MSA.

See the *Cisco Threat Response User Guide* for the setup procedure and for more information.

Setting up the MSA for Cisco IDS 4.0

The MSA converts SNMP traps into the ManHunt event format and sends these events over EDP.

Setting up the MSA for Cisco IDS 4.0 involves two steps:

- Installing the MSA for Cisco IDS 4.0
- Configuring the MSA for Cisco IDS 4.0

Installing the MSA for Cisco IDS 4.0

You can deploy the MSA for Cisco in either of two deployment modes:

- Install the MSA on a dedicated host (recommended)
- Install the MSA on the same host as the ManHunt node

In either deployment, the MSA listens for Cisco SNMP traps on port `162` by default. The MSA converts the SNMP traps into the ManHunt event format and sends the events to ManHunt over EDP. During the MSA installation or configuration, you specify the IP address of the ManHunt node that will receive the event data from the MSA. The MSA and ManHunt node communicate over EDP. To do so, they must share an EDP passphrase to ensure secure and encrypted communication.

See "Changing the EDP passphrase" on page 11.

Note: The EDP for Symantec ManHunt 2.2 patch 2 has an event rate limitation of `50` events per second, and the EDP for Symantec ManHunt 3.0 has an event rate limitation of `250` events per second. Please note the ManHunt event rate limit when planning multiple MSA deployments.

Note: Log on as root to run the install script. In the installation log, which is located in the `<MSA_install_dir>/install` directory, you can view the ManHunt version number and third party MSA product name and version number.

To install the MSA for Cisco IDS 4.0

1. Place the CD in the CD-ROM drive; mount the drive if necessary.
2. Change to the CD directory, and run the following command:

   ```
   cd Cisco40MSA_MH<version>/install/<platform>
   ```

   where `<version>` is `22` or `30`, and `<platform>` is `linux`, `solaris8-intel`, or `solaris8-sparc`.
3. Run the following command:

   ```
   ./install.sh
   ```

4. Do one of the following:
   - Type a directory where you want to install the MSA.
   - Accept the default `/usr/msacisco` directory, and press **Enter**.
5. Do one of the following:
   - Type a directory to which the MSA will write the operational log files.
   - Accept the default `<MSA_install_dir>/logs` directory, and press **Enter**.

Note: The MSA cannot start properly if the log file approaches a certain size (2-3 GB depending on the system). You can delete or rename the log file to correct the problem.

6 Type the ManHunt host IP address, and press **Enter**.

This is the IP address of the ManHunt node that will accept the Cisco event data.

7 Do one of the following:

- Type the EDP port number used by this ManHunt node.
- Accept the default port number of `1333`, and press **Enter**.

This port number must match the value for the EDP Port Number configuration parameter used by the ManHunt node that will receive the Cisco event data.

8 Type the EDP passphrase, and press **Enter**.

Note: The MSA for Cisco communicates with the ManHunt node over EDP. In order to enable ManHunt to receive event data from the MSA for Cisco, they must share an EDP passphrase. This must be identical to the passphrase that you enter in the ManHunt console when you create the external sensor node for the MSA for Cisco. The passphrase must be 8-64 characters long, inclusive.

See “Changing the EDP passphrase” on page 11.

9 Re-enter the EDP passphrase, and press **Enter**.

This ends the installation.

10 Change to the MSA installation directory, and run the start command to start the MSA for Cisco:

```
<MSA_install_dir>/start
```

Configuring the MSA for Cisco IDS 4.0

The MSA installation process creates a configuration file called `cisco2mh.conf` in the `<MSA_install_dir>/etc` directory. This file contains instructions and parameters for MSA operation and for connecting to the ManHunt node. These parameters are described in Table 1-1.

MSA Configuration File

The configuration file is divided into sections with section headers enclosed in brackets [ ]. The first section is called `[MSA]` and contains most of the configuration parameters. The second section is called `[Snmp]` and can contain the SnmpTrapPort and SNMPListenIP parameters.

The following is a sample configuration file:

```
[MSA]
    ManHuntHostIPAddr = 10.0.0.34:1333
    EDPSecret = DokdYjNU732mnDuj
    MSALogDir = /usr/msacisco/logs
    MSALogLevel = 5
    EventDefinitionFile = /usr/msacisco/etc/cisco2mh.evtdef
[Snmp]
SnmpTrapPort = 185
```

Table 1-1 lists all editable parameters. If you edit any of the configuration parameter values, you must restart the MSA application.

See “Starting and stopping the MSA” on page 11.

Table 1-1 MSA Configuration File Parameters

Parameter	Description
EDPSecret	This is the value for EDPSecret, and it is the encrypted form of the EDP passphrase. It is set during the MSA installation process. Do not attempt to edit this parameter from within the configuration file. **Note:** This parameter is required.
EventDefinitionFile	This is the path to the event definition file. The MSA conversion engine uses instructions contained in the event definition file to convert Cisco events into ManHunt events. The event definition file is installed in the `<MSA_install_dir>/etc` directory. **Note:** This parameter is required.
EventSendRate	This is an integer specifying the maximum number of events per second that can be passed to the ManHunt node. Valid values are `10-250` for ManHunt 3.0 and `10-50` for ManHunt 2.2. If this parameter is not specified in the configuration file, the default value is `10` events per second. To change the default value for this parameter, you must add it to the `[MSA]` section. **Note:** The MSA cannot start properly if the log file approaches a certain size (2-3 GB depending on the system). You can delete or rename the log file to correct the problem.
ManHuntHostIPAddr	This is the IP address of the ManHunt node to which Cisco events are sent. The format is `IP address:port`. The port must be the port on which ManHunt is configured to receive events. The default port is `1333`. If you change the EDP Port Number parameter on the ManHunt node, be sure to change the value in the MSA configuration file to match, and vice versa. **Note:** This parameter is required.

Table 1-1 MSA Configuration File Parameters

Parameter	Description
MaxEventsinCache	This is an integer specifying the maximum number of events allowed in the cache before the oldest event is dropped. Valid values are `500-100,000`. If this parameter is not specified in the configuration file, the default value is `3000`. To change the default value for this parameter, you must add it to the `[MSA]` section.
MSALogDir	This is the directory to which the MSA should write its log file. The default value is `<MSA_install_dir>/logs`. If you delete this parameter from the configuration file, then the default log directory becomes `/tmp`.
MSALogLevel	This is an integer specifying the level of logging that the MSA uses. Possible values are from `1` to `35`, with `35` being the most verbose. The default value is `5`. If you raise the log level above `5`, the performance of the MSA for Cisco may be negatively impacted.
SNMPListenIP	This is a valid IP address to which the MSA machine is bound.
SnmpTrapPort	This is an argument that allows SNMP traps to be collected on a port other than the default, which is port `162`.

Note: It is possible to install and run two SNMP-based MSAs on the same computer. However, that computer must have more than one IP address. Each MSA will have a separate `.conf` file in which each `SNMPListenIP` parameter must be set to a different value.

Warning: If you have only one IP address on the computer and are already running an application that uses the SNMP ports, any SNMP based MSA, such as the MSA for Cisco IDS 4.0, will not start. The MSA will exit immediately without any indication. To verify a running MSA, run the following command: `ps -a | grep cisco2mh`. You should see the `cisco2mh` file running.

Managing the MSA for Cisco IDS 4.0

Within the MSA for Cisco, you can start and stop the MSA, view events in the log file, and change the EDP passphrase.

Starting and stopping the MSA

The MSA installer creates startup scripts in the system startup directories `/etc/init.d` and `/etc/rc2.d` to automatically start the MSA for Cisco when the machine is rebooted. In addition, the `<MSA_install_dir>` directory provides start and stop scripts. You must log on as root to run these scripts. Simply run the `start` or `stop` commands from `<MSA_install_dir>` to start or stop the MSA.

Viewing Cisco events in the ManHunt console

You can view events from the MSA for Cisco just as you would view any other events in the ManHunt console.

For more information about viewing events in the ManHunt console, see the *Symantec ManHunt Administration Guide.*

To identify events as originating from Cisco

- In the ManHunt console Event View window, expand the **Base Type** field.
  - Cisco events have a Base Type in the following format:

    `CISCO|<cisco event name>`
  - The **Type** field in the ManHunt console contains a short description of the Cisco event

To see more information, double click on the event and click the **Advanced** tab.

Changing the EDP passphrase

To change the EDP passphrase on the ManHunt node, edit the external sensor object in the topology tree. The EDP passphrase on the ManHunt node must match the EDP passphrase on the MSA for Cisco host. Therefore, if you change the passphrase on the ManHunt node, you must also change the passphrase on the MSA for Cisco host by running the `changesecret` command located in the `<MSA_install_ directory>/bin` directory. When you finish changing the passphrase, restart the MSA.

See “Starting and stopping the MSA” on page 11.

Changing the EDP passphrase on the ManHunt node

You can change the EDP passphrase on the ManHunt node through the external sensor object in the topology tree. If you change the EDP passphrase on the ManHunt node, you must also change the passphrase on the MSA for Cisco host.

To change the EDP passphrase on the ManHunt node

1. In the ManHunt console, right-click the appropriate external sensor object, and select **Edit**.
2. In Edit External Sensor, click **Set EDP Passphrase**.
3. In EDP Passphrase, enter the new passphrase the ManHunt node will use to communicate with the MSA for Cisco.

   The passphrase must be between 8-64 characters long.
4. Re-enter the passphrase for confirmation.
5. Click **OK**.
6. In Edit External Sensor, click **OK**.
7. Click **Topology** > **Save Changes**.

Note: If the EDP passphrase element does not appear active, use the `edppwd` tool in the `<MH inst directory>/tools` directory to change the passphrase.

Changing the EDP passphrase on the MSA for Cisco host

The EDP passphrase on the ManHunt node must match the EDP passphrase on the MSA for Cisco host. Therefore, if you change the EDP passphrase on the ManHunt node, you must also change the passphrase on the MSA for Cisco host.

To change the EDP passphrase on the MSA for Cisco host

1. Go to the `<MSA_install_dir>/bin` directory.
2. Enter the following command:

   ```
   changesecret <MSA_install_dir>/etc/cisco2mh.conf
   ```
3. Enter the old passphrase.
4. Enter the new passphrase. The passphrase must be at least 8 characters long.
5. Re-enter the new passphrase.
6. Restart the MSA application with the stop and start commands.

See “Starting and stopping the MSA” on page 11.

Note: If you have forgotten the old passphrase, you can delete the `EDPSecret` line from the configuration file `<MSA_install_dir>/etc/cisco2mh.conf` and then run `changesecret` again. The script will not prompt you for the old passphrase after the passphrase line is removed.

See “Configuring the MSA for Cisco IDS 4.0” on page 7.

Uninstalling the MSA for Cisco IDS 4.0

You can uninstall the MSA for Cisco without uninstalling the Cisco meta data. However, if you require more space on the disk after uninstalling the MSA for Cisco, you can remove the meta data manually by deleting the `<ManHunt_install_directory>/md/cisco.md` file.

To uninstall the MSA for Cisco IDS 4.0

1. Run the following command:

   ```
   <MSA_install_dir>/install/uninstall.sh
   ```

2. To continue uninstalling the MSA for Cisco, type `y` and press **Enter**.